Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

2019 Hanwha Techwin S-Cert Team

NVR Vulnerability Report

■ OVERVIEW

- Vulnerability : Buffer overflow (CVE-2019-12223)
- Description

  The listed NVR is vulnerable to allow remote attackers to cause a denial of service (such as system crash and reboot) using buffer overflow.

■ AFFECTED PRODUCTS AND FIRMWARE

Model	Firmware Version	Status	Remarks
SRN-1000	v1.52 and earlier versions	No plan	Discontinued
SRN-1670D	V2.04 and earlier versions	No plan	Discontinued
SRN-470D	V2.04 and earlier versions	No plan	Discontinued
SRN-1673S	v1.16 and earlier versions	Ongoing (V1.18_1909XX)	Discontinued
SRN-873S	v1.16 and earlier versions	Ongoing (V1.18_1909XX)	Discontinued
SRN-473S	v1.16 and earlier versions	Ongoing (V1.18_1909XX)	Discontinued
SRN-472S	v1.06 and earlier versions	Resolved (1.08_190614)	Discontinued
SRN-4000	V2.20 and earlier versions	Ongoing (V2.22_1909XX)	Discontinued

■ RISK ANALYSIS

Vulnerability	Review Result	Severity
Buffer overflow (CVE-2019-12223)	The NVR can be rebooted via external attack continuously if it can be access via the public network. Also, Vulnerability is quite easy to attack if knowing simple skills.	High

■ Current Status & Plan

Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

- Already, Hanwha Techwin have released patched firmware regarding SRN-472 only.
- The listed all models are currently discontinued. Nevertheless, the patched firmware of SRN-1673S, 873S, 473S, 4000 model is being prepared until end of September.
- However, SRN-1000, 1670D, 470D models are not able to release patched firmware any more due to being discontinued long ago.

■ Required Action

- If patched firmware exists, update NVR immediately.
  If not, NVR needs to be disconnected from the public network or be blocked from untrusted IPs using IP firewall.